 Doc 1

UNITED STATES DISTRICT COURT

for the

District of New Hampshire

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Campus Convenience, 152 Winchester Street, Keene, New Hampshire

Case No. 1-21-mj-56-01-15

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Please see attachment A-5.

located in the _____ District of New Hampshire, there is now concealed *(identify the person or describe the property to be seized)*:

Please see attachment B-5.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1960, 371	- Prohibition of Unlicensed Money Transmitting Business and Conspiracy
18 U.S.C. §§ 1343, 1349	- Conspiracy to Commit Wire Fraud, and Wire Fraud
18 U.S.C. § 1956(a)	- Laundering of Monetary Instruments Including Funds Represented to be Proceeds of Specified Unlawful Activity

The application is based on these facts:

Please see attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Kathryn Thibault
Applicant's signature

Special Agent Kathryn Thibault, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by **Telephonic conference** *(specify reliable electronic means).*

Date: 03/15/2021

Andrea K. Johnstone
Judge's signature

City and state: Concord, New Hampshire

Hon. Andrea K. Johnstone, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Kathryn Thibault, being duly sworn, hereby depose and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), reporting to the Boston, Massachusetts Division, and have been employed by the FBI since October 1998. I am currently assigned to the Bedford Resident Agency of the FBI and am assigned to work primarily on white collar crime cases. I am familiar with the tactics, methods and techniques of people who commit bank fraud, wire fraud, money laundering and violations of regulations relating to money services businesses. I have attended numerous federal agency and private sponsored training courses. In June 2017, I attended an on-line networking and enterprise training conference in Atlanta, Georgia where cryptocurrency, use of e-mail in money laundering cases and the dark web were topics of instruction. I have participated in financial investigations, and am aware of how targets use the financial system to launder proceeds of illegal activities. As a Special Agent with the FBI, I am responsible for conducting criminal investigations involving violations of Title 18 of the United States Code and other federal statutes enforced by the FBI.

2. In addition, in conducting this investigation and preparing this affidavit, I have consulted with FBI personnel who have substantial expertise investigating crimes involving virtual currency. I have worked closely with FBI analysts who are assigned to FBI Headquarters on the Virtual Currency Evolving Threats (VCET) Team. Specifically, I have worked with two analysts who, as part of their duties at the FBI, have participated in complex international investigations into money laundering facilitators, cyber criminals, national and transnational criminal enterprises, organized crime, and violent crimes. They have extensive experience investigating criminal organizations that leverage virtual assets to launder illicit proceeds, to include violations involving money laundering and operating an unlicensed money transmitting business. Through the course of these investigations, they have advised on investigative strategy, analyzed financial flows, reviewed legal process, and affected virtual asset seizures. They have

also provided training to federal and international law enforcement partners and prosecutorial authorities and participated in numerous virtual currency conferences. Statements in this affidavit regarding virtual currency and the law surrounding virtual currency are based in part on my own knowledge and in part on my conversations and consultation with them.

II. PURPOSE OF THE AFFIDAVIT

3. This affidavit is submitted in support of an application for a search warrant for evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1960, 371 (prohibition of unlicensed money transmitting business and conspiracy), 18 U.S.C. §§ 1343, 1349 (conspiracy to commit wire fraud and wire fraud), 18 U.S.C. § 1956(a) (laundering of monetary instruments, including funds represented to be proceeds of specified unlawful activity), 31 U.S.C. §§ 5313(a) and 5322 (failure to file currency transaction reports ("CTRs")), and 31 U.S.C. § 5318(h) and 5322 (failure to maintain an effective anti-money laundering program) (collectively, the "Subject Offenses"). As set forth below, there is probable cause to search for evidence, contraband, fruits, and instrumentalities of these offenses, as set forth in **ATTACHMENTS B-1 through B-15** at the premises described in **ATTACHMENTS A-1 through A-15** (hereby incorporated).

4. On or about March 15, 2021, a federal Grand Jury in the District of New Hampshire returned an indictment charging Ian Freeman ("Freeman"), Colleen Fordham ("Fordham"), Renee Spinella ("R. Spinella"), Andrew Spinella ("A. Spinella"), No First Name Nobody ("Nobody") and Aria DiMezzo ("DiMezzo") with conspiracy to operate an unlicensed money transmitting business in violation of Title 18 United States Code Sections 371, 1960(a), and 1960(b)(1)(B). The indictment charges Freeman, Fordham, R. Spinella, A. Spinella and Nobody with conspiracy to commit wire fraud in violation of Title 18, United States Code, Sections 1343 and 1349 and wire fraud and Freeman with operating a continuing financial crimes enterprise in violation of Title 18 United States Code Section 225 and money laundering in violation of Title 18 United States Code Sections 1956(a)(3)(B). It also charges DiMezzo and Freeman with operating an unlicensed money transmitting business. Accordingly, given the

Grand Jury's determination of probable cause, this affidavit will present an overview of the investigation and allegations with respect to these individuals while focusing on facts giving rise to probable cause to support the issuance of search warrants for the specified locations and persons which, investigators believe, will yield evidence of criminal activity, contraband, and fruits and instrumentalities of these crimes.

5. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not purport to set forth all of my knowledge of or investigation into this matter.

III. PREMISES TO BE SEARCHED

6. The premises to be searched, more fully described in Attachments A-1 to A-15, which are incorporated by reference and included as though fully set forth herein are:

SUBJECT PREMISES	LOCATION
A-1	73-75 Leverett Street, Keene, New Hampshire
A-2	Bitcoin Embassy aka Mighty Moose Mart (formerly Route 101 Goods), 661 Marlboro Street, Keene, New Hampshire
A-3	142 Chester Rd., Derry, New Hampshire
A-4	788 Alstead Center Rd., Alstead, New Hampshire
A-5	Keene Convenience, 152 Winchester St., Keene, New Hampshire (Location containing an ATM operated by Freeman)
A-6	Murphy's Taproom, 494 Elm St., Manchester, New Hampshire (Location containing an ATM operated by Freeman)
A-7	659 Marlboro Street, Keene, New Hampshire
A-8	Red Arrow Diner, 149 Daniel Webster Highway, Nashua, New Hampshire (Location containing an ATM operated by Freeman)

A-9	Person of Aria DiMezzo
A-10	Person of Colleen Fordham
A-11	Person of Ian Freeman
A-12	Person of Nobody
A-13	Person of Renee Spinella
A-14	Person of Andrew Spinella
A-15	Person of Christopher Rietmann

7. A-1 describes the residences of Freeman and Nobody, A-2 describes a business used by Freeman, Fordham, Christopher Rietmann ("Rietmann") and co-conspirators, A-3 describes the residence of R. Spinella and A. Spinella, A-4 describes the residence of Fordham, A-7 describes the residence of DiMezzo, and A-5, A-6, and A-8 are businesses where cryptocurrency ATMs (sometimes called cryptocurrency kiosks or vending machines) operated by Freeman and his co-conspirators are located. The government seeks warrants to seize only the kiosks and related instrumentalities, including their cash contents, at the various business locations described in A-5, A-6, and A-8.

IV. BACKGROUND ON VIRTUAL CURRENCY

8. Virtual currency (also known as virtual assets, cryptocurrency, or digital currency, for purposes of this affidavit) is generally defined as an electronic-sourced unit of value that can be used as a substitute for fiat currency (i.e., currency created and regulated by a government). Examples of cryptocurrency are Bitcoin, Bitcoin Cash, Dash, Monero, and Ether. Virtual currency exists on the Internet, in electronic storage devices, or in cloud-based servers. Virtual currency is not issued by any government, bank, or company and is instead often generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the

decentralized network, containing an immutable and historical record of every transaction.[1] Virtual currency is not illegal in the United States and may be used for legitimate financial transactions. However, virtual currency is often used for conducting illegal transactions, such as the sale of controlled substances.

9. Bitcoin is a type of virtual currency. Bitcoin payments are recorded on a public ledger that is maintained by peer-to-peer verification, and is thus not maintained by a single administrator or entity. Individuals can acquire Bitcoins either by "mining" or by purchasing Bitcoins from other individuals. An individual can "mine" for Bitcoins by allowing his/her computing power to verify and record the Bitcoin payments into a public ledger. Individuals are rewarded for this by being given newly created Bitcoins.

10. An individual can send and receive Bitcoins through peer-to-peer digital transactions or by using a third-party broker. Specifically, individuals can acquire bitcoin through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people. Such transactions can be done on any type of computer, including laptop computers and smart phones.

11. Bitcoins are stored in digital "wallets." A digital wallet essentially stores the access code that allows an individual to conduct Bitcoin transactions on the public ledger. To access bitcoins on the public ledger, an individual must use a public address and a private key. The public address can be analogized to an account number while the private key is like the password to access that account. A public address is represented as a case-sensitive string of letters and numbers, 26–35 characters long or a lowercase string of letters and numbers beginning with the prefix "bc1q." Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address' private key can authorize any

[1] Some cryptocurrencies, like Monero, operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

transfers of cryptocurrency from that address to another cryptocurrency address. When sending Bitcoin to a public address, an individual may also scan a "QR" code (i.e., a barcode) that contains the address, for easier transmission of that address.

12. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Ledger).

13. Wallets can also be backed up with a "recovery seed," sometimes called a "root key" or "seed key." Recovery seeds are word sequences that represent (encode) a random number used as a seed to derive a wallet. The sequence of words is the wallet backup and can recover and re-create the wallet and all the derived keys in the same or any compatible wallet application.

14. Wallets, represented through recovery seeds and/or private keys, can be backed up into many forms, for example, paper printouts, USB drives, word processing files, or CDs. Additional security safeguards for cryptocurrency wallets can include a complex password and/or two-factor authorization (such as a password and a phrase). Individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

15. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device ("private wallets"). A user typically accesses the private wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

16. All Bitcoin transactions are recorded on a public ledger known as the "Blockchain," stored on the peer-to-peer network on which the Bitcoin system operates. The Blockchain serves to prevent a user from spending the same Bitcoins more than once. However, the Blockchain only reflects the movement of funds between anonymous Bitcoin addresses and, therefore, cannot by itself be used to determine the identities of the persons involved in the transactions. Only if one knows the identities associated with each Bitcoin address involved in a set of transactions is it possible to meaningfully trace funds through the system.

17. Even though the public addresses of those engaging in Bitcoin transactions are recorded on the public ledger, the true identities of the individuals or entities behind the public addresses are not recorded. If, however, a real individual or entity is linked to a public address, it would be possible to determine what transactions were conducted by that individual or entity.

Bitcoin transactions are, therefore, described as "pseudonymous," meaning they are partially anonymous.

18. Although cryptocurrencies such as bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering, and is an oft-used means of payment for illegal goods and services on hidden services websites operating on the Dark Web, websites accessible only through encrypted means. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track purchases within the Dark Web marketplaces. Through the Dark Web or Darknet, i.e., websites accessible only through encrypted means, individuals have established online marketplaces, such as the Silk Road, for narcotics and other illegal items. These markets often only accept payment through virtual currencies, such as Bitcoin. Accordingly, large amounts of Bitcoin sales or purchases by an individual can be an indicator that the individual is involved in narcotics trafficking or the distribution of other illegal items. Individuals intending to purchase illegal items on Silk Road-like websites need to purchase or barter for Bitcoins. Further, individuals who have received Bitcoins as proceeds of illegal sales on Silk Road-like websites need to sell their Bitcoins to convert them to fiat (government-backed) currency.

19. Such illicit purchases and sales are often facilitated by peer-to-peer Bitcoin exchangers, who are not registered with the federal or a state government, or by exchangers that offer a degree of anonymity. These unregistered exchangers often charge a higher transaction fee than legitimate, registered virtual currency exchangers who have robust anti money-laundering programs, including full customer verification.[2] This higher fee is essentially a premium that the unregistered exchangers charge in return for not filing reports on exchanges pursuant to the Bank Secrecy Act, such as Currency Transaction Reports and Suspicious Activity

[2] Based on my training and experience, I am aware that one of the largest U.S.-based (and registered) virtual currency exchanges, Coinbase, charges approximately 2-3% commission per transaction.

Reports. Peer-to-peer Bitcoin exchangers can conduct these transactions in person or through technology, such as cryptocurrency ATMs (described below).

V. BACKGROUND ON VIRTUAL CURRENCY AND FINCEN/BSA REGULATIONS

20. Based on my training and experience and the investigation to date, I am aware that exchangers of virtual currency are considered money transmitters under federal law. Specifically, I am aware of the following:

a. The Bank Secrecy Act ("BSA") is codified at 31 U.S.C. §§ 5313-5326. These laws were enacted by Congress to combat the use of financial institutions to launder the proceeds of crime. 31 U.S.C. § 310 establishes the Financial Crimes Enforcement Network ("FinCEN") as a bureau within the Treasury Department, and describes FinCEN's powers and duties to, among other things, enforce compliance with the BSA.

b. The definition of a financial institution under the statute, 31 U.S.C. § 5312(a)(2)(R), includes "a licensed sender of money or any other person who engages as a business in the transmission of funds[.]" Under the relevant federal regulations, financial institutions are also defined as "money servicing businesses," ("MSBs") which include "money transmitters." See 31 C.F.R. § 1010.100(t)(3) (defining "financial institution" as a "money servicing business"); 31 C.F.R. § 1010.100(ff)(5) (defining money transmitters as money services businesses).

c. In 2013, FinCEN issued guidance that a money transmitter can include an individual who offers exchange services between virtual currency and fiat currency. See Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001, issued March 18, 2013 (the "FinCEN Guidance"). This guidance was reaffirmed in May 2019. The FinCEN Guidance articulated that those who are money transmitters because they offer exchange services between virtual currency and fiat currency are also MSBs and must comply with the applicable portions of the BSA, some of which are described below.

d. Federal regulations exempt several categories of business and services from the definition of money transmitter, including communication service providers, payment processors, physical currency transporters (such as armored car services), prepaid access card providers, and individuals who transmit funds integral to the sale of goods or provision of services. 31 C.F.R. § 1010.100(ff)(5)(ii)(A)-(F). None of these exemptions would apply to a digital currency exchanger, such as Freeman and his associates, as described below.

e. Financial institutions, including MSBs and money transmitters, are required to report each deposit, withdrawal, exchange of currency, or other payment or transfer involving more than $10,000 in currency. See 31 C.F.R. §§ 1022.300, 1022.310, 1022.311, and 1022.312 (cross-referencing 31 C.F.R. §§ 1010.300, 1010.310, and 1010.311, and 1010.312); see also 31 U.S.C. § 5313(a). These reports are referred to as Currency Transaction Reports ("CTRs"). A "transaction" for purpose of filing a CTR includes "multiple currency transactions . . . if the financial institution has knowledge that they are by or on behalf of any person and result in either cash in or cash out totaling more than $10,000 during any one business day." 31 C.F.R. § 1010.313. CTRs must be filed within 15 days following the day on which the reportable transactions occurred. See 31 C.F.R. § 1010.306(a)(1). Financial institutions must verify and record the name and address of the individual who conducted the reportable transactions, and must accurately record the identity, social security number, or taxpayer identification number of any person or entity on whose behalf the reportable transaction was conducted. See 31 C.F.R. § 1010.312. CTRs are filed with FinCEN and are made available to law enforcement. It is a federal crime under Title 31 for an MSB or money transmitter to fail to file a CTR. See 31 U.S.C. §§ 5313(a) and 5322.

f. In addition to being required to file CTRs, certain MSBs, including money transmitters, are required to file suspicious activity reports ("SARs"). See 31 C.F.R. §§ 1022.320 (stating at sub-section (a)(1) that money transmitters are a type of MSB required to file SARs). SARs must be filed on transactions aggregating to at least $2,000 in value and the MSB knows or has reason to suspect: (1) the funds are derived from illegal activity or are intended to hide or

disguise funds or assets derived from illegal activity to violate or evade any federal law or regulation; (2) the transaction is designed to evade the Title 31 reporting requirements; (3) the transaction services no apparent business or lawful purpose, and there is no other reasonable explanation for the transaction; and (4) the transaction involves use of the money transmitter to facilitate criminal activity. See 31 C.F.R. §§ 1022.320(a)(2)(i)-(iv). MSBs are required to file a SAR within 30 calendar days after the date of the initial detection of the underlying facts that warrant the filing of a SAR. See 31 C.F.R. §§ 1022.320(b)(3). Lastly, MSBs are required to maintain supporting documentation for the SAR for a period of five years from the date of filing the SAR. See 31 C.F.R. §§ 1022.320(c). It is a federal crime under Title 31 for a money transmitter to fail to file a SAR. See 31 U.S.C. §§ 5318(g) and 5322.

g. Financial institutions, including MSBs and money transmitters, are required to create and maintain effective anti-money laundering compliance programs. See 31 U.S.C. § 5318(h)(1); see also 31 C.F.R. § 1010.210. The program must have written policies, procedures, and controls governing the verification of customer identification, the filing of reports such as CTRs, the creation and retention of records, responses to law enforcement requests, and other compliance with BSA requirements. The anti-money laundering compliance program must have a compliance officer who is responsible for assuring that the business complies with all BSA requirements. It is a federal crime under Title 31 for an MSB or money transmitter to fail to maintain an effective anti-money laundering compliance program. See 31 U.S.C. §§ 5318(h)(1) and 5322.

h. Any person who owns or controls an MSB is responsible for registering, and periodically re-registering, the business with FinCEN. See, 31 U.S.C. § 5330(a); see also 31 C.F.R. § 1022.380. Registration must be done on or before the end of the 180-day period beginning on the day following the date the business was established. See, 31 C.F.R. § 1022.380(b)(3). A money transmitting business that fails to register with FinCEN is subject to criminal liability under 18 U.S.C. § 1960. Specifically, § 1960 makes criminally liable anyone who "knowingly conducts, controls, manages, supervises, directs, or owns all or part of an

unlicensed money transmitting business." That includes, under 18 U.S.C. § 1960(b)(1)(B), a business that "fails to comply with the money transmitting business registration requirements under section 5330 of title 31, United States Code, or regulations prescribed under such section[.]"

i. Additionally, even if a money transmitter is registered with FinCEN, 18 U.S.C. § 1960(b)(1)(C) also criminalizes money transmitting businesses that "involve . . . the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity."

VI. BACKGROUND ON CRYPTOCURRENCY AUTOMATED TELLER MACHINES

21. Based on my training and experience, I am aware of the following.

22. Cryptocurrency ATMs are electronic terminals that act as mechanical agencies of the owner-operator, to enable the owner-operator to facilitate the exchange of cryptocurrency for currency or other cryptocurrency. Many types of cryptocurrencies may be purchased through cryptocurrency ATMs (and in fact the ATMs discussed in this warrant sell different types of cryptocurrencies including Bitcoin, Bitcoin Cash, Dash and Monero). These cryptocurrency ATMs may connect directly to a separate exchanger, which performs the actual cryptocurrency transmission, or they may draw upon the cryptocurrency in the possession of the owner-operator of the electronic terminal. In this investigation, Freeman used his own cryptocurrency accounts to provide exchange services. Thus, a transactor at the ATM need not have an account with Freeman or any connection to Freeman in order to obtain or sell cryptocurrency.

23. Under FinCEN's guidance (FIN-2019-G001, May 2019, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf), an owner-operator of a cryptocurrency ATM who uses an electronic terminal to accept currency from a customer and transmit the equivalent value in cryptocurrency (or vice versa) qualifies as a money transmitter both for transactions receiving and dispensing currency.

24. Cryptocurrency ATMs often look like traditional banking ATMs and can contain some of the same physical features as a regular bank ATM such as: a touch screen, keypad, cash dispenser, receipt printer, cash and/or card reader, and are generally free-standing machines. These features allow crypto ATMs to accept cash for payment, in exchange for cryptocurrency, which is transferred to the cryptocurrency address of the user's choice. The kiosk generally gives a paper receipt that contains the details of the transfer. Cryptocurrency ATMs can also take cryptocurrency and provide a user with cash, but I believe this feature has been disabled on the ATMs at issue in this case.

25. Cryptocurrency ATMs are secured with external locks to both the machine itself and to the internal cash boxes. Inside the ATM is usually a built-in computer system or digital tablet configured to run software to facilitate transactions. The hardware and software maintain computer logs, like any regular computer or tablet, related to the operating system, software applications, and transactional data. Cryptocurrency ATMs allow the owner/operator to attach a keyboard to the computer or tablet to interact with the operating system and software for administrative purposes.

V. SUMMARY OF PROBABLE CAUSE

26. In 2017, the FBI, Internal Revenue Service ("IRS"), and the United States Postal Inspection Service ("USPIS") initiated an investigation of Freeman and his associates and their virtual currency-fiat cash exchange business. The investigation has revealed that since at least 2015, Freeman has operated an unlawful money services business ("MSB") selling millions of dollars in virtual currency. By operating an unlicensed MSB, Freeman sells virtual currency without abiding by any FinCEN and Bank Secrecy Act regulations which require MSBs to, among other things, have an anti-money laundering program, file SARs and CTRs, and collect know-your-customer information. Freeman runs his business through purported religious organizations that he and his co-conspirators have founded including the Shire Free Church, the Crypto Church of NH, the Church of the Invisible Hand, the NH Peace Church, and the Reformed Satanic Church. In order to mislead banking institutions and prevent them from

identifying the business as an MSB, Freeman and his co-conspirators engage in a series of lies and omissions, most commonly describing deposits into bank accounts for virtual currency purchases as "church donations" and transfers of money to buy virtual currency as "church outreach." Freeman also uses personal bank accounts to run his business and instructs co-conspirators to open bank accounts in their names for his use.

27. Freeman and others sell virtual currency in two ways. They advertise on peer-to-peer virtual currency trading websites, such as LocalBitcoins.com ("LBC") and Paxful.com, where they accept bank deposits, wires, or cash sent by mail in exchange for cryptocurrency.[3] They also operate various cryptocurrency ATMs. Freeman generally charges a 5% to 15% or higher fee for transactions – which is significantly higher than what a customer is charged by a regulated virtual currency exchange that complies with U.S. anti-money laundering laws, such as Coinbase. As of March 6, 2021, FinCEN records confirmed that Freeman, his co-conspirators, and the entities they operate have not registered with FinCEN as an MSB in violation of 18 U.S.C. § 1960(b)(1)(B).

28. Freeman is very careful about making clear that virtual currency clients should not tell him what they do with their money. In fact, on the ATMs, he posted instructions which clearly state, "do not tell our staff why you want the coins" and on his LBC profile he wrote, "what you do with your bitcoin is your business. Don't tell me what your plans are. If you do, I reserve the right to refuse the sale." Nevertheless, law enforcement has learned that criminal actors who use virtual currency to further their crimes have successfully exploited Freeman's business for separate criminal pursuits, often involving online scams and fraud.

VI. STATEMENT OF PROBABLE CAUSE

The Shire Free Church, Shire Cryptocurrency Vending, and Other Church Entities

[3] Localbitcoins.com is a peer to peer Bitcoin exchange. It is an online marketplace where individuals can buy, sell and trade Bitcoin with each other. The site allows users to post advertisements where they state exchange rates and payment methods for buying or selling bitcoins. The advertisements allow clients to reply to these advertisements and agree to meet in person to buy bitcoins with cash, or trade directly with online banking. I know that Paxful is a global cryptocurrency trading platform that operates like localbitcoins.com.

29. The Shire Free Church appears to be the original of various related churches operated by this group. The articles of agreement filed on December 12, 2013, lists board members Darryl Perry, Ian Freeman, Mark Edgington, Wendy French, and Jason Denonville. As of 2018, documentation states that only Freeman, Perry, and Edgington remain board members. The incorporation documents state that, "the corporation will assist the ministers in their mission fostering peace by facilitating interactions with the people calling themselves 'the state' regarding serving the community through positive action for charitable, educational, and religious purposes. This corporation is established to appease whatever arbitrary and nebulous dictates handed down by whichever monopolistic violent governmental agency may turn its capricious attention towards the Shire Free Church, its people, and/or any of its ministers, while we go about the good work of spreading the ideas of human freedom and morality." The address of the church is 73 Leverett Street (Subject Premises A-1).

30. According to its website, the church operates "Shire Cryptocurrency Vending." The website states that the goal of the organization is not to profit but to foster peace, the mission of the church. It continues that funds earned are invested in cryptocurrency outreach and other church outreach projects. It also states that the group operates vending machines in the Keene college area, Route 101 in Keene, and Murphy's Taproom in Manchester. I believe these refer to the ATMs described in A-5, A-2, and A-6 respectively. The website also describes the ATMs as "vending machines," which this group claims makes them different from ATMs because they do not connect directly to cryptocurrency exchanges and therefore do not require "ridiculous identification requirements." One of the machines operated by Shire Cryptocurrency Vending is located at the "Bitcoin Embassy," the premises described in A-2. According to its website, "the Bitcoin Embassy of New Hampshire provides education, networking opportunities and innovation in decentralized digital assets, blockchain technologies and more."[4]

[4] Freeman also listed the address of the Bitcoin Embassy (Subject Premises A-2) as the address of the most recent church I identified him to operate. Christopher Rietmann's LinkedIn profile lists him as the executive director of the Bitcoin Embassy. The Bitcoin Embassy is located in a store, previously named Route 101 Goods, recently renamed "Mighty Moose Mart" that houses the ATM but also sells virtual currency paraphernalia, food, and other goods.

31. Co-conspirators have registered additional churches in their names as well. In 2017, R. Spinella founded the Crypto Church of NH which she registered with the New Hampshire Secretary of State. She listed the church address as 73 Leverett Street (Subject Premises A-1). In 2019, Nobody filed an application for trade name for the "Church of the Invisible Hand" with business address of 73 Leverett Street (Subject Premises A-1) as a "church or religious organization." On the application he also listed his address as 75 Leverett Street (also Subject Premises A-1). Freeman is listed as the payer and filer on this form with the New Hampshire Department of State. In 2020, DiMezzo (under her previous name of James Baker) applied for a trade name of Reformed Satanic Church, a "religious and community outreach organization" with the state of New Hampshire, with an address of 659 Marlboro street (Subject Premises A-7), a residence directly adjacent and on the same property as the Bitcoin Embassy (Subject Premises A-2). In July 2020, Freeman registered the trade name "NH Peace Church" with its purpose "OTHER / religious" with its principal office listed as 661 Marlboro Street (Subject Premises A-2) and mailing address of a P.O. box used by Freeman.

Fraud Victims and Freeman's Bank Accounts

32. The investigation into Freeman began because law enforcement agencies across the country identified suspicious funds, often determined to be criminal proceeds, being deposited into accounts operated by Freeman and his associates, including accounts in the name of the church entities previously discussed. Many deposits included notes describing the deposits as "church donations." FBI Agents and other law enforcement officers around the United States interviewed individuals who deposited money into those bank accounts and determined that many of these individuals were victims of online scams of various types. Notably, some people interviewed said they willingly deposited money into Freeman's bank account in order to purchase bitcoin and were not victims of any scams. However, none of the individuals interviewed stated that their purpose in sending money to Freeman was to donate money to a church. The following are representative samples of some interviews the FBI conducted:

a. On May 16, 2019, an FBI agent interviewed S.D. at S.D.'s residence in Ohio. S.D. is a widow who, after the death of her husband in July 2017, started an online relationship with a David Brusch who told her that he was going to purchase diamonds in South Africa. Brusch convinced S.D. to "get cash and forward it to people to buy Bitcoin." When shown a copy of a $25,000 transfer she made to "Ian Freeman," S.D. said this transfer of money was done at Brusch's direction. S.D. does not know Freeman or the Shire Free Church.

b. On May 5, 2019, an FBI agent interviewed J.C. at J.C.'s residence in North Carolina. J.C. said that she met Adam Karlsson on match.com in June 2018. At Karlsson's direction, she subsequently sent money to "Ian Freeman" to "help" Karlsson and in return for his promise to come to North Carolina and have a relationship with her. J.C. deposited a total of $36,000 in Freeman's bank account. J.C. stated that Karlsson "swindled" her out of her money. J.C. does not know Freeman or the Shire Free Church.

c. On July 15, 2019, an FBI agent interviewed D.B. at D.B.'s residence in Ohio. He recalled that in 2017, he was scammed out of money on multiple occasions and as part of the scam he specifically remembered sending money to the Shire Free Church. This scheme involved fraudulent "investments" and D.B. was instructed by the scammers online to send money to the Shire Free Church to "cover attorney fees." D.B. does not know Freeman or the Shire Free Church.

d. On July 15, 2019, an FBI agent interviewed K.C.at K.C.'s residence in Tennessee. Earlier in 2019, K.C. was involved in a lottery scheme where she was instructed by scammers to open a bank account at SunTrust Bank. K.C. received checks from the scammers who instructed her to send the funds from these checks to "Ian Freeman." K.C. then sent money to Freeman at Axos Bank. K.C. does not know Freeman or the Shire Free Church.

e. On April 14, 2018, an FBI agent interviewed M.F. at a business near her residence in Michigan. In approximately March 2018, M.F. was contacted by a

David Brusch, whom she met through an online dating website. Eventually M.F.'s relationship with Brusch became romantic, although she never met him in person. Brusch asked M.F. to transfer him money so it could "clear customs." On one occasion, Brusch instructed M.F. to transfer some of this money to an account bearing the name, "Shire Free Church." M.F. knows now that Brusch scammed her into making these transfers and sending him her money. M.F. does not know Freeman or the Shire Free Church.

f. On September 5, 2018, an FBI agent interviewed S.E. at S.E.'s residence in New Hampshire. S.E. met Michael Burnam through Facebook and started an online romantic relationship with him that, at the time of the interview, had lasted about five years. Michael asked S.E. to accept wire transfers from him and then move this money to other accounts. For example, Michael asked S.E. to accept cash that he mailed to her, approximately $25,000, and then instructed her on how to use Freeman's bitcoin ATMs to convert this cash to bitcoin. He specifically directly S.E. to use the ATM located at Uncommon Goods in Keene, NH (former name of Subject Premises A-2). S.E. does not know Freeman or the Shire Free Church.

g. In late 2018, a medical doctor who lives in Alabama, D.T., fell victim to a scheme where he was told to send money to help a friend who had been arrested. D.T. sent $4,020.13 to a bank account in the name of "Colleen Fordham." After realizing he was the victim of a scam, D.T. filed a police report with his local department, and due to the investigation, the bank froze the $4,012.13 in Fordham's account until this matter could be resolved. On January 9, 2019, the investigating police officer received a call from a male who identified himself as "Ian Freeman from the Shire Free Church in Keene, New Hampshire." Freeman claimed to be representing Colleen Fordham and inquired about the issue. The officer's report states in part, "[f]rom speaking with Freeman, he seemed to have direct knowledge of the situation, specifically the reported fraud associated with the account. Freeman said that Fordham initially

believed the check was sent legitimately in exchange for Bitcoin. Freeman said he would set up a time for the officer to talk to Fordham." GFA Credit Union ended up returning the $4,012.13 to D.T. after Colleen Fordham, through her attorney, gave a notarized statement to GFA Credit Union acknowledging the fraudulent activity on her account.

h. In September 2020, P.B. in Texas received a fraudulent email purporting to be from the Federal Housing Administration and Federal Trade Commission saying that his identity had been compromised and requesting he make payments to purchase bitcoin to, among other places, an account opened by Freeman in the name NH Peace Church. He was instructed to write "reason for wire: donation." An investigator spoke to Freeman who confirmed he owned the account and said he was a bitcoin broker, though denied knowledge of the fraud which led P.B. to make the purchase.

33. After learning of these and other fraudulent deposits into bank accounts, investigators received bank records for accounts used by Freeman and associated churches, and a search warrant for email accounts used by Freeman and co-conspirators. Investigators also used an undercover officer to purchase bitcoin from Freeman.

Undercover Officer ("UC") & Money Laundering

34. Beginning around the fall of 2019, a UC began conducting bitcoin purchases from Freeman after finding him on LBC. On September 11, 2019, Freeman instructed the UC to deposit money into Colleen Fordham's personal checking account at TD Bank ending 2980. The UC was required to send a note saying "I certify I am buying bitcoin from the Shire Free Church." The UC deposited approximately $500 and received bitcoin in exchange.

35. On or about November 13, 2019, the UC requested to purchase bitcoin and Freeman directed him to deposit into a First Tech Credit Union personal checking account in Freeman's name ending 8014. The UC deposited approximately $500 and received bitcoin in exchange.

36. After the first few purchases, Freeman directed the UC to contact him via Telegram, an encrypted messaging service. He told the UC that he charges 12% for cash deposits and has a $500 minimum. He said that his friend "Pope Nobody" could handle smaller trades and that they "work together." I know that Nobody also uses the moniker Pope Nobody.

37. On or about November 15, 2019, the UC contacted Freeman to purchase bitcoin and Freeman directed him to deposit into his First Tech Credit Union Account 8014 and told him to write as the reason for the deposit "Purchase of Rare Coins / Investment." The UC deposited approximately $500 and received bitcoin in exchange.

38. On or about March 17, 2020, the UC contacted Freeman asking if he was still selling Bitcoin. Freeman responded that he has "CHASE for cash deposit . . . also can do Wire . . . cash by mail." He continued, "Sales are brisk . . . I can handle a lot per day – what do you need? I have plenty of coin on hand." The UC responded that he would need up to $20,000 and when asked how he would pay said, "I may do each method to spread out if you know what I mean." When asked about which account to use, Freeman explained that, "the last credit union froze my account." When asked why, Freeman responded, "All banks and CUs will close cash deposit accounts eventually. I've lost dozens of accounts over four years. They don't like cash deposits coming in from all over. It's not illegal, but they can get in hot water with the regulators over it."

39. On April 8, 2020, the UC contacted Freeman to initiate a purchase. Freeman told him to send the money to JP Morgan Chase Bank Account 9038, account name, "Church of the Invisible Hand" with the reason for the deposit "Church donation" and Church Address as 73 Leverett St in Keene, (Subject Premises A-1). Nobody is the only authorized signatory on this account, which was opened by him in January 2020 listing 73 Leverett St. as the address. The UC deposited $3,000 and Freeman deposited $2,639.45 worth of bitcoin to the UC's wallet. The UC explained to Freeman, "I mainly deal with cash" and "I'm just trying to get rid of cash lol."

40. On or about April 24, 2020, the UC contacted Freeman about another possible purchase. This time Freeman said Chase closed his account and directed him to the Church of the

Invisible Hand account at Bank of America 9633, reason for deposit: church donation. In March 2020, Nobody opened and was the only authorized signatory on this account as well.

41. On May 5, 2020, the UC contacted Freeman for another purchase. Freeman instructed him to mail a check to Ian Freeman at 63 Emerald Street #610. The UC sent a check for $5,000. Freeman then told the UC that after depositing the check but before it cleared, his account had been locked, saying "this shit always happens eventually with bank accounts." He was very apologetic. Because of the delay, Freeman told the UC that he would thereafter permanently reduce his fee to 10%. On May 20, 2020, the UC received $4,339.47 in bitcoin.

42. On or about May 29, 2020, the UC reached out to Freeman about meeting up for a transaction and Freeman responded "I am sadly, not selling at this time due to losing two bank accounts." On or about June 6, 2020, Freeman told the UC that his friend Aria was accepting wires and money orders "if you'd like to trade with her, please let me know and I will introduce you." Aria is DiMezzo's first name.

43. On or about June 19, 2020, Freeman said he was still on hold with Chase but directed the UC to the "vending machine at Thirsty Owl." I know that at the time, Freeman operated a virtual currency ATM at a bar called the Thirsty Owl in Keene, New Hampshire. Freeman instructed the UC to let him know when he arrived so that he could reduce the machine's rate from 14% to 10%. Freeman admitted that he had the rate higher "the last couple weeks due to banking/exchange issues." The UC explained, "I have $11k to get rid of, don't want it to be too suspicious with that much cash. Want to hang out around town without the cash if you know what I mean." Freeman responded, "We've had old ladies go there and drop $40k in that location." Freeman continued that, "no ID or phone required to use it, since it's a private sale of BTC." The UC responded, "I just don't want any forms filed on me if you know what I mean." Freeman responded, "oh, no way -we have disabled all that nonsense. . . All ID factors are turned off. It is a private wallet-to-wallet sale, not money transmission like most machines do."

44. When the UC arrived, the machine appeared out of service. The UC contacted Freeman who in turn called the Thirsty Owl and the owner apologized and turned on the machine. Freeman lowered the rate to 10%. As the machine only accepted $5,000 at a time, the UC asked what to about the additional $6,000. Freeman instructed him to start another purchase clarifying that there was no limit to how many purchases he could make. The UC ultimately conducted three transactions, two for $5,000 and one for $1,000. He received bitcoin from a wallet affiliated with Freeman (discussed below).

45. After the purchase at the Thirsty Owl, the UC met with Freeman on the town green in Keene. Freeman introduced the UC as his "long time crypto client." Nobody and DiMezzo were also at the meeting. During the meeting, Freeman offered the UC marijuana and the UC said he has better stuff and that he sells heroin and MDMA. Freeman said he doesn't do heroin but maybe could use the MDMA. Freeman told the UC not to tell anyone what the UC does. Although the conversation was recorded, there is a lot of cross talk, and this part of the conversation is inaudible.

46. On or about July 30, 2020, the UC reached out again requesting to purchase $20,000. Freeman responded as follows (only excerpts of the text message conversation are included below and quotes included in this affidavit are approximate):

> FREEMAN: Thank you, I enjoyed meeting you and don't want to be rude, but unfortunately I can't sell you bitcoin because you told me too much about what you do. As you probably know, I'm not opposed to your line of work, but I can't knowingly help you with financial matters. I hope you can understand.
>
> UC: Bummer... I thought I had the perfect connection lol, wish I didn't say anything now . . . I thought I only told you about cars which is my main thing. Can't even use your ATM?
>
> FREEMAN: My answer to the question is – I can't KNOWINGLY assist you with financial matters... You told me you sell drugs. Therefore to assist you with buying bitcoin would be considered money laundering. Money laundering requires knowledge of the illegal activity. I don't think you're an undercover agent but you got a little too loose lipped, so while I am not opposed to the sale of drugs, I do need to be careful. Sadly that means I cannot KNOWINGLY sell bitcoin to you. Nearly every bitcoin seller the feds have taken down have sold to an undercover stating they did something illegal to get the money. It's just not worth the risk to me.
>
> UC: Those appear to be serious accusations, I mean money laundering words, I'm not well knowledgeable with these laws as you are, but I can see where you're coming from. I just though

no big deal about selling some drugs to let you know that, since you're open minded about that stuff. I myself always have to watch out for feds too.

47. Freeman nevertheless invited the UC to still attend the bitcoin meetups in Keene. On or about August 25, 2020, the UC went to a meetup in Keene with Freeman and others. At the end of the meeting, the UC and others had the following conversation (only excerpts included):

UC:	Thirsty Owl open today?
FREEMAN:	Yeah, every day.
MALE VOICE:	[interposing] Okay. What's the closest Bitcoin vending machine?
UC:	I actually got to go to one too.
MALE VOICE:	You can put dollars in and get Bitcoin out - -.
MALE VOICE:	How do you get Bitcoin out? Is it like a--
FREEMAN:	[Interposing] If you want to do it without an ID you'd have to go to Keene.
UC:	It's like an ATM machine.
MALE VOICE:	Code or something?
MALE VOICE:	What's that?
MALE VOICE:	Do you get a code?
MALE VOICE:	You put your wallet, cash inside, and it goes in a wallet.
MALE VOICE:	- - or nothing in addition - -.
MALE VOICE:	Also, I just learned that I should buy some Bitcoins, very seldom, three weeks later, then you make profits.
UC:	Depends if it goes up again, yeah.
MALE VOICE:	Do you pay like captain gains?
FREEMAN:	Only if you're a sucker.
[Laughter]	
MALE VOICE:	Yeah - -.
MALE VOICE:	Yeah, don't buy through an exchange. Don't buy through any place that asks for a social security number or an ID.
[Crosstalk]	
[Background Noise]	
MALE VOICE:	Yeah, thanks for coming, guys.
UC:	I was gonna swing by and maybe show him - -.
FREEMAN:	You can just meet us there, yeah.
UC:	Can I use it?
FREEMAN:	I can't tell you that you can't use that.

UC:	Okay.
FREEMAN:	Okay?
UC:	All right. Thanks, man. I was - -.
UC:	I'm gonna go to the--I have some cash. I want to put into Bitcoin. So I'm gonna use the ATM machine.
MALE VOICE:	Okay.

48. The UC went to the Thirsty Owl where he conducted four approximately $5,000 deposits and received approximately $17,033.76 in bitcoin from the same wallet affiliated with Freeman as the last purchase there.

Freeman's Knowledge of MSB Requirements

49. From as early as 2016, Freeman has been directly informed by banks and virtual currency exchanges that his sales of virtual currency and operation of cryptocurrency ATMs meets the legal definition of an MSB. For example, in July 2016, Freeman tried to open an account with virtual currency exchange Gemini in the name of the Shire Free Church. Gemini researched the church and identified Freeman's ATM business, at that time called "Shire Bitcoin Vending." They asked whether he would be using Gemini to source any of the ATMs. Freeman responded, "Shire Bitcoin Vending is one of many projects of the church" and that "Gemini could be used as a source for bitcoins that eventually could end up in a bitcoin vending machine as inventory." On July 14, 2016, Gemini responded, "We do believe Shire Bitcoin Vending would be considered an MSB and therefore should be registered with FinCEN and maintain an AML policy." Gemini declined to open an account for Freeman. Emails show that other financial institutions told Freeman the same thing.

50. In 2017, Freeman provided another virtual currency exchange who determined that his ATM business made him an MSB, with a letter from an attorney stating his opinion that Freeman is not an MSB under state or federal law. The letter is dated November 2017. The theory relied on by the attorney, which Freeman frequently advocates, is that because his ATMs do not connect directly to a virtual currency exchange and are funded by private wallets Freeman controls, he is simply conducting a private sale of a good through a vending machine. He says

that he is therefore not operating as an MSB. The attorney letter provides an opinion only about the ATM business and not Freeman's broader virtual currency sales business. I am aware, based on my training and experience, that operators of unlicensed money service businesses frequently claim that they are not MSBs because they do not transmit money to third parties. I have consulted with FinCEN who have explained that the attorney's opinion and this claim is wrong.

51. In fact, on July 13, 2018, about eight months after Freeman received the opinion from his attorney, FinCEN informed Freeman of this fact. FinCEN sent a letter and email (recovered in more than one email account Freeman operated) notifying him that FinCEN "believes that your business is a money services business as defined by the BSA." The letter explained that Freeman was required to register with FinCEN and comply with anti-money laundering, record-keeping, and reporting regulations. The letter provided that if Freeman disagreed with the characterization of his business as an MSB, he should contact FinCEN within two weeks with an explanation. FinCEN confirmed that Freeman never contacted them and to date has not registered his business.

52. Freeman did not apparently change any business practices after receiving the FinCEN letter. Through the beginning of 2020 (when email search warrant returns were received), he continued to send out the 2017 attorney letter and make the same arguments about why he is not an MSB. Notably, it does not appear that many banks or exchanges were convinced by Freeman's arguments as they generally refused to do business with him or closed his accounts as soon as the nature of his business came to light. Various email exchanges recovered pursuant to the search warrant also show that other cryptocurrency investors disagreed with Freeman's arguments about the law. For example, on July 24, 2018, another investor provided Freeman with an analysis by his attorney about how FinCEN defines MSBs telling him, "Yes, by FinCEN's interpretation, any exchange of one currency for a virtual currency makes one a money transmitter." He also sent Freeman FinCEN's guidance on how they enforce MSB laws when it comes to virtual currencies.

Freeman's Banking Activity

53. Financial records show that Freeman generally operates two sets of bank accounts. Some accounts receive cash deposits, checks, and wires from virtual currency customers. These accounts can be easily identified because they receive frequent wires and/or deposits at bank branches across the United States (often multiple deposits in one day at various different bank branches), an activity consistent with virtual currency for cash sales. Often times, the memo lines on deposited checks or the reasons for the wire read "church donation." Investigators have identified over 20 bank accounts used by Freeman and co-conspirators in this manner.

54. After receiving money into his accounts from customers, Freeman aggregates the deposits from the first set of accounts and writes large checks to other accounts he controls. The memo line on these checks frequently reads "church outreach." Money in this second set of accounts is then used to purchase virtual currency from exchanges. I believe that Freeman operates these two sets of accounts to obfuscate the nature of his business. In one email to virtual currency exchange Bittrex on January 25, 2019, Freeman explained, "I send wires from my AXOS account which is funded by checks from the Cheshire County Federal Credit Union which is funded by local deposits from my church. The funds are allocated to me to purchase bitcoin for investment purposes."

55. Freeman has openly discussed the fact that banks frequently shut his accounts down when they learn about the nature of his business. In a November 2019 email, he wrote:"[I]f I mention virtual currency like bitcoin up front, no bank or credit union will open an account for me so I have to keep quiet and hope they leave me alone. Eventually, they notice the large wires, look at the destination, see a virtual currency exchange, and then close my account. I've had it happen to business accounts for my church, of which I am a minister, and also to my personal accounts. I prefer to wire from my personal accounts . . . at the Kraken exchange. This month I have sent over 1.8 million USD in wires and my current credit union is shutting me down." In an October 29, 2019, email with Silvergate Bank (who refused to open an account for him because of the "risk" involved in supporting his business), Freeman wrote, "[i]t's no fun

having to skulk about the banking world, continuing to lose accounts randomly once banks decide they don't like sending wires to bitcoin exchanges. I've done it for half a decade successfully, but it sure would be nice to have somewhere to bank that's not scared or hostile ... is the risk of which you speak the risk of unwanted government attention and potential fines that could come from banking for crypto vending operations?" At one point, Freeman specifically reached out to Walpole Bank, explaining the nature of his business to them and telling them "so far no bank or credit union is knowingly willing to have us as clients."

56. An analysis of Freeman's bank accounts confirms that he has engaged in a pattern of making false or misleading statements to banks when he opens accounts or when the banks question the purpose of his accounts. He has also used co-conspirators to operate bank accounts for him. Members of this conspiracy also open personal accounts but use them primarily for the virtual currency exchange business.

57. The most frequent story that Freeman presents to the banks is that he is a minister of a church and that he is opening accounts to receive church donations and conduct church outreach. He has opened various accounts in the name of the Shire Free Church. In 2020, he opened at least one bank account in the name NH Peace Church with himself as a signatory, which account received deposits for the bitcoin business through at least the end of January 2021. Often, Freeman instructs customers to either write on their check memo lines or provide as the reason for the deposit or wire if asked at the bank, "church donation." Customers interviewed by the FBI would testify that they deposited into Freeman's accounts to purchase virtual currency and were not making donations to the church. When asked by banks about these deposits, Freeman (and his co-conspirators who open accounts on his behalf) frequently repeated the false statement that the deposits were church donations.

58. For example, in May 2016, Freeman applied for a business account for the Shire Free Church Monadnock at Service Credit Union. On the application, Freeman answered "no" to the following questions: (1) Does the business transmit currency on behalf of customers and (2) Does the business sell currency or perform currency exchanges. Bank statements indicate that the

account was used for bitcoin customers from across the country to deposit money. On April 13, 2017, bank representative David Long called Freeman to update the bank's "Business Information Card" and discuss why the account was receiving deposits from shared banking branches across the country. Freeman falsely told Long that "the funds are from people all over the country donating to the church services," that all deposits were related to the Shire Free Church, and that Freeman reaches "donors" across the country through his radio show.

A. Spinella, R. Spinella & Subject Premises A-3

59. On April 3, 2018, the FBI interviewed A. Spinella. A. Spinella explained that R. Spinella[5] worked for Freeman and is a close friend of Freeman. He explained that in December 2017, Freeman asked A. Spinella to open accounts in A. Spinella's name at Wells Fargo, Bank of America and itBit, also known as Paxos Trust, (a virtual currency exchange) because Freeman could no longer open accounts in his own name. A. Spinella opened the accounts, but did not use them for his personal banking. He said that Freeman had explained that one account would be used for check deposits and another to write checks. A. Spinella was given a book of checks that Freeman asked him to sign and turn over to him. A. Spinella did so, and Freeman took over the accounts.

60. A. Spinella believed that Freeman used the accounts to purchase and sell Bitcoin. A. Spinella told the agents that R. Spinella also sold Bitcoin for Freeman on LBC. He believed she is compensated with 10% of any profit.[6] A. Spinella said that Freeman buys the Bitcoin at a low price and profits from the sales and that his business name has the word "church" in it. A. Spinella said he signed checks for Freeman two or three times per week. He authenticated his signature on checks payable to Freeman from his bank accounts.

---

[5] A. Spinella and R. Spinella were not married at the time, and R. Spinella's maiden name is Renee LeBlanc. Various of the accounts opened in her name were in her maiden name, though she will be referred to only as R. Spinella in this affidavit.

[6] I have reviewed emails between R. Spinella and Freeman that confirm their business relationship, and list amounts of cryptocurrency on loan to R. Spinella.

61. Bank records show that A. Spinella's Wells Fargo account (8055) was opened on November 28, 2017 and shows cash deposits from across the country consistent with virtual currency purchases. A. Spinella's Bank of America ("BOA") account was opened on November 11, 2017. Records show checks written from the Wells Fargo account to the BOA account. Between January 25, 2018, and April 2, 2018, $108,450 in outgoing wire transfers were made to itBit, a virtual currency exchange from the BOA account. This is consistent with Freeman's use of two sets of bank accounts previously discussed.

62. R. Spinella has also opened numerous accounts used by Freeman both at banks and virtual currency exchanges. For example, she opened an account at virtual currency exchange Gemini in 2017, listing her occupation as homemaker. When questioned about all the money going through the account she wrote, "I don't have job but I do work at home for myself with money that has been loaned to me." When further questioned, she explained, "I have a private loan from a local church whose ministers I know well. They trust me and helped by providing me funds so I could continue to work from home rather than go back to a job." The account was closed.

63. In 2017, R. Spinella founded the "Crypto Church of New Hampshire." The incorporation documents for the Crypto Church of NH list the address as 73 Leverett Street in Keene (Subject Premises A-1). The object/purpose of the corporation on the NH articles of agreement filed November 17, 2017, states: "To further the Church's mission of spreading peace in accordance with our prophet's great vision, which was inspired by God. Our actions in furtherance of this divine mission are for charitable, educational, and religious purposes." The only board members are R. Spinella and Christopher Rietmann (who I believe works at the Bitcoin Embassy, Subject Premises A-2 and lives at Subject Premises A-4). R. Spinella then opened an account at itBit in the name of the church, providing as the mission of her business: "to further the church's mission of spreading peace in accordance with our prophet's great vision, which was inspired by God." She described the source of funds for the account as "donations."

64. R. Spinella and A. Spinella reside at Subject Premises A-3. On her 2017 application for the itBit account, R. Spinella listed the registered mailing address of the business as 73 Leverett Street (Subject Premises A-1) but the physical location address of the church as Subject Premises A-3. She listed Subject Premises A-3 as the address of the church on a 2018 Kraken application as well. I therefore believe that evidence of her use of the Crypto Church of NH (or other churches) to conduct the unlawful virtual currency exchange business will be found at that location.

65. R. Spinella has also opened various bank accounts in her name, using the address of Subject Premises A-3, as recently as the fall of 2020. The accounts opened by R. Spinella operate the same way as the accounts run by Freeman do. They include many frequent deposits at different bank branches from virtual currency customers across the country. In many of the accounts, funds are then aggregated and R. Spinella writes large checks to Freeman for deposit into his other accounts, indicating that she uses the accounts for the virtual currency exchange business.

66. For example, on January 11, 2018, Freeman and R. Spinella went to Service Credit Union and opened a business account in the name Crypto Church of NH with R. Spinella as the signer, listing 73 Leverett as the residence (Subject Premises A-1). R. Spinella answered "no" to the following application questions: (1) Does the business transmit currency on behalf of customers and (2) Does the business sell currency or perform currency exchanges. She included the following responses: "Major customers: International Ministry" and the bank included the comment, "online ministry that has members internationally." The bank employee who opened the account noted that Freeman provided answers to many of the questions. When asked if he would be on the account, he said no and that he was "just a member of the church." R. Spinella explained that the "church was a universal church and that donations would be coming in from all over the world. That is where the cash expectancy of $100k is coming from." On March 12, 2018, Freeman brought a check written from Chris Rietmann's Route 101 Goods (Subject Premises A-2's former name) bank account for $20,000 with the notation, "church donation" and

deposited it into the account. In addition, some of the checks A. Spinella signed for Freeman were also deposited into the account.

67. I believe that records of R. Spinella and A. Spinella's participation in the virtual currency exchange business, financial records of profits earned from the business and cryptocurrency, and employment relationship with Freeman as well as other evidence of the crimes under investigation would be found at the premises and on electronic devices they each use.

Colleen Fordham, Christopher Rietmann & Subject Premises A-4

68. I also believe that Fordham has worked for Freeman in a similar role as R. Spinella. Specifically, she has described herself as a "contracted payment processor." In November 2018, GFA bank investigator April English contacted Fordham about a fraudulent deposit into her account. Fordham told her that the deposit was for a purchase of "rare coins." When questioned further, in subsequent communication with the bank on December 12, 2018, Fordham stated that she was a contracted agent of the non-profit Shire Free Church that engages in the sale of bitcoin as part of the church's mission to foster peace. She explained "my role as the Church's agent in this process is as a payment facilitator." As a result of the suspicious circumstances, the bank contacted the local police who called Fordham to inquire about the deposit. Fordham again stated that she is the "payment facilitator for the Shire Free Church" and allows her account to be used by the church to process online bitcoin sales. After Fordham hung up from the detective, Freeman called the detective, said he represented Fordham, and wanted to know what the detective needed from her.

69. The bank informed Fordham that they would be closing her account and she provided them with an "Agreement to Assist Shire Bitcoin's Outreach Operations with Banking Support" which described her as a contracted payment processor for the Shire Free Church. They also provided a letter from an attorney stating that Fordham was not operating as a money transmitter because she works as a payment processor for Freeman.

70. Various accounts opened in Fordham's name were used for Freeman's virtual currency exchange business. For example, the account that Freeman instructed the UC to deposit money into (ending 2980) was a personal account opened in Fordham's name, with Subject Premises #4 as the listed address, on September 27, 2018. From that date to October 2019 when it was closed, the account received $2,240,431.94 in deposits from across the country and made $2,042,563 in payments to Freeman's other accounts, $242,627 wired and $1,799,936 via checks. Correspondence with TD Bank confirmed that Fordham operated this account for Freeman. On or about September 24, 2019, according to investigator Kathy Beshey she spoke to Fordham over the phone about a fraudulent deposit into the account and Fordham stated that she "sold rare coins and invested in rare coins." When asked if she shipped the rare coins to customers, Fordham stated she was only the bookkeeper to the business. Beshey explained that because the account was opened as a personal account it would be restricted from any business transactions and the account would be closed. Shortly after they hung up, Freeman called and though Beshey said she couldn't discuss details of the account with him, he asked for her title, name and contact information. On October 2, 2019, Freeman sent a letter explaining that Colleen serves as a "contracted payment processor who assists me, as part of my church mission, in selling Bitcoin online to buyers around the country." This account was closed by the bank in October 2019.

71. Rietmann and Fordham are also signatories on various bank accounts in the name of Route 101 Goods, the former name of the business that now serves as the Bitcoin Embassy. These bank accounts wrote large checks and made deposits into accounts operated by Freeman and used for the virtual currency exchange business. In 2019, an FBI UC observed both Fordham and Christopher Rietmann working at the store/Bitcoin Embassy described in A-2. I believe that Rietmann and Fordham have operated the business together. I also believe that Fordham and Rietmann are in a long-term relationship and that they both reside at Subject Premises A-4. They both have current registrations with the New Hampshire DMV at that address. I believe that records of their virtual currency exchange business, the ATM located at the Bitcoin Embassy,

financial records of profits earned from the business and cryptocurrency, and employment relationship with Freeman as well as other evidence of the crimes under investigation would be found at the premises and on electronic devices they each use. I also know that Rietmann's name is on the trade name documents for one of the churches opened by R. Spinella and that associated records may also be found as well.

Aria DiMezzo & Subject Premises A-7

72. Aria DiMezzo has identified herself as the High Priestess of the Reformed Satanic Church, an affiliate of the Shire Free Church, also operates accounts used similarly. In July 2020, U.S. Postal Inspectors ("Inspectors") in North Carolina identified suspicious parcels, believed to contain large amounts of cash, being sent from Donald Zofrea, a retired school groundskeeper living in Knightdale, NC to Freeman. Inspectors confronted Zofrea about the packages, their contents, and the reason for them being sent. Shortly thereafter, in August 2020, Inspectors noticed an envelope sent from Freeman to Zofrea, interdicted it, and asked to speak with Zofrea about it. Zofrea gave consent to search the parcel, which contained a cashier's check for $50,000 written off of Zofrea's bank account to the Reformed Satanic Church being mailed from Freeman back to Zofrea. Zofrea admitted that he had been helping a woman he met on an online dating website to purchase bitcoin. Zofrea stated that he had been sending money to Ian Freeman and his wife "Kelly" to purchase bitcoin on behalf of a woman he met online. Zofrea had opened a bank account on behalf of the woman who would deposit money into the account and then ask Zofrea to send it to Freeman. On this occasion, Freeman's "wife" had told him to send the check to "Ari Dimazza." I believe this to refer to DiMezzo. Apparently, DiMezzo could not purchase enough bitcoin to fund the sale and was therefore sending the check back to Zofrea. Exchange records indicate that DiMezzo has sent bitcoin to the same virtual currency wallet used by Freeman (the "Holding Wallet" discussed below).

73. DiMezzo also posted a YouTube training video on how to sell bitcoin on LBC. In the video, filmed at the Bitcoin Embassy, she discusses the substantial profits she makes and gives instruction on how to maximize those profits. She explains that one of the biggest

challenges is that banks will inevitably close her accounts, emphasizing, "it's a matter of when, not if." She advised, when discussing how to get banks to keep the accounts open longer, "fewer interactions with human beings is best. Humans will be curious what you're doing. Automated systems don't care." She also explained that because she sells bitcoin on behalf of a church, she does not have to pay taxes.

74. I believe that DiMezzo resides at 659 Marlboro Street (Subject Premises A-7). She has paid utilities at that location as recently as records are available, January 2021. The Reformed Satanic Church trade name documents list this as the address for the church. In addition, bank records in the name of the church with DiMezzo as the only signer list this as the address. Paxos Trust records also list this as the address on file for accounts in the name of James Baker (DiMezzo's former name) and the institutional account for the Reformed Satanic Church. A vehicle registered to James Baker has been parked overnight at this address as recently as the night of March 10, 2021. The post office that delivers mail to the address confirmed that another individual who I have not linked to this investigation has received mail at the address during the week of March 7, 2021.

Nobody, Freeman, and 73-75 Leverett Street Residence (Subject Premises A-1)

75. An analysis of bank records has confirmed that Nobody in the name of the Church of the Invisible Hand has opened bank accounts used by Freeman for his bitcoin business as well. The accounts he opened show deposits from across the country, consistent with virtual currency purchases, frequently with "church donation" as the reason for the deposit, and then large checks/wires out of the accounts to Ian Freeman. In addition, as discussed previously, Freeman instructed a UC buying bitcoin from him to make a deposit into two of Nobody's accounts.

76. Freeman resides at 73 Leverett Street in Keene, New Hampshire and has this as his registered address. According to the City of Keene, New Hampshire Property and Tax Assessment Department this address, 73-75 Leverett Street in Keene is a duplex. This property was originally purchased by Ian Bernard (Freeman's former name) on May 19, 2006. In 2014,

Freeman transferred ownership of the property to the Shire Free Church Monadnock. Freeman also operates a nightly radio show, Free Talk Live, or FTL from 73 Leverett Street, which contains a recording studio. Various people visit the residence to record and/or participate in the radio show.

77. According to records from the NH DMV, seven people including Freeman have registered addresses at 73 Leverett Street. Seven people including Nobody have registered addresses at 75 Leverett Street. Freeman is the only name on the utility bill for both 73 and 75 Leverett street as recently as January 2021, the most recent date for which records are available. A car used by Nobody is frequently parked overnight outside Leverett street and has been there as recently as March 10, 2021 and I believe 75 Leverett Street to be his primary residence. The post office that delivers mail to the residence confirmed that there was mail addressed to Ian Freeman as well as at least two others at 73 Leverett street during the week of March 7, 2021. The post office confirmed that there was mail addressed to Nobody and at least one other person at 75 Leverett street during the week of March 7, 2021.

78. Investigators who monitored a fixed camera outside the residence in 2019 observed various people coming and going but this review has not allowed me to determine currently whether others regularly live at each residence. I have also observed various surveillance cameras located outside the residences. I know that reviewing data from these cameras may allow me to identify co-conspirators and whether packages coming and going from the residence are affiliated with the business discussed herein.

79. I know that Freeman operates a postal box at the Shipping Shack in Keene, New Hampshire but that he also receives packages at 73 Leverett Street. I believe that Freeman has sent and received cash through the mail. Sometimes, he has mailed cash out to purchase virtual currency. I am aware of an investigation by federal agents in Texas who identified a package with $71,000 dollars sent from Freeman with a note saying, "Ian Freeman is purchasing bitcoin."

80. As Nobody and Freeman reside in each side of the duplex, as the property is owned by the church used to facilitate this crime, as Freeman pays utilities for both sides, and for

the reasons discussed throughout this affidavit, there is probable cause to believe that both parts of the residence will contain evidence and proceeds of the crimes discussed herein.

Profits from the Scheme

81. Despite frequently stating that he is not operating a "business" and that the church operates a non-profit, there is substantial evidence that Freeman and his co-conspirators profit greatly from their scheme. Whereas legitimate exchanges, like Coinbase and Gemini, typically charge fees of less than 2 percent, Freeman's fees (both at ATMs and from LBC sales) range from 5 to 14 percent. Notably, the only benefit Freeman offers over a legitimate exchange is anonymity and refusal to file SARs and CTRs.[7] Freeman is well aware that the lack of AML/KYC policies is an asset to his business as he frequently touts the "privacy" he offers to prospective customers.

82. Freeman also has stated that he is "a minister of a church and hence do[es] not receive a paycheck" and has not received one since 2004. He has not filed taxes since at least 2015. Likewise, Freeman's co-conspirators have either not filed taxes or report minimal income compared to the profits made from this business. One exchange requested a letter from an accountant detailing Freeman's assets and in March 2018, he provided a letter stating that he had $300,000 in bank accounts, and $2.4 million in other assets. Identified virtual currency wallets associated with Freeman have current balances worth substantially in excess of $1,000,000.

Operation of Virtual Currency ATMs

83. According to records from U.S. Customs and Border Protection ("CBP") reviewed by FBI analysts in Washington, D.C., at least eight cryptocurrency ATMs have been imported to New Hampshire and received by entities or individuals associated with Freeman. Currently, I believe that Freeman operates at least four ATMs.

84. On March 6, 2021, I reviewed the website for Shire Cryptocurrency vending. The website includes addresses for three ATMs operated by the group (though Freeman refers to

[7] An IRS agent reviewed FinCEN databases and was not able to locate any SARs or CTRs filed by Freeman as of March 2021.

them as "vending machines"): at Campus Convenience in Keene (Subject Premises A-5), the Bitcoin Embassy New Hampshire (Subject Premises A-2), and Murphy's Taproom in Manchester, New Hampshire (Subject Premises A-6). It also states that Dash, Bitcoin, Bitcoin Cash and Monero are available at the cryptocurrency ATMs located at the Bitcoin Embassy in Keene (Subject Premises A-2) and Murphy's Tap Room in Manchester (Subject Premises A-6).

85. I also reviewed coinatmradar.com on March 6, 2021. Based on my review of email accounts used by Freeman, I know that he frequently updates the information on his ATMs with the website. Additionally, the Shire Cryptocurrency Vending website also contains a link to coinatmradar.com as a place to "track the status of NH's Cryptocurrency Vending Machines." The ATMs identified above are on this website with "Bitcoin Embassy New Hampshire" as the operator. In addition, the ATM located at the Red Arrow Diner in Nashua also lists "Bitcoin Embassy New Hampshire as the operator (Subject Premises A-8).

86. The devices are wall mounted at the Red Arrow Diner and Murphy's Tap Room. The wall mounted devices are accessed by a key on the right side of the device that will open the right panel and allow access for the wall mount to be removed. The stand-alone cryptocurrency ATMs are located at the Bitcoin Embassy, and Campus Convenience. The stand-alone devices are bolted to a floor for security purposes and are accessed with a key to open the system and remove the mount. All devices have a key that physically open the internal compartments to remove the cash.

87. As detailed below, FBI Agents used U.S. currency to make purchases of virtual currency at all of the cryptocurrency ATMs. FBI analysts have linked those kiosks to each other and to Freeman based on the following analysis.

88. Between February 25, 2016, and March 2, 2021, the following virtual asset service provider (VASP) accounts (also referred to in this affidavit as exchanges) withdrew a

total of approximately 6,458.67 bitcoin directly to various bitcoin addresses. Based on co-spend analysis[8], all these addresses belong to the same wallet (herein, "Holding Wallet"):

VASP	Accountholder	Account Identifier Ending	Approximate Bitcoin Amount Sent to Holding Wallet
Bittrex	Ian B Freeman	3b2b3bf419f5	40.8
Coinbase	Shire Free Church/Ian Bernard	0003	519
Coinbase	Shire Free Church Monadnock/Ian Freeman	0001dc	154
Gemini Trust	Ian Freeman	250	30
Gemini Trust	Renee LeBlanc	473	119
Payward Ventures, Inc.	Ian Freeman	BY2I	1,747
LocalBitcoins	FTL_Ian/IAN B FREEMAN	FTL_Ian	48
LocalBitcoins	ShireBTC/IAN B FREEMAN	ShireBTC	6.5
Paxful	Ian Freeman	FTL_Ian	17.74
Paxos Trust	Andrew Spinella	0389	12
Paxos Trust	Ian Freeman	3904	1,860
Paxos Trust	Shire Free Church Monadnock/Ian Freeman	1514	1,731
Paxos Trust	Renee LeBlanc	6670	102
Paxos Trust	James Baker/Aria DiMezzo	ff895e5072c2	42
Paxos Trust	Reformed Satanic Church/James Baker	505b749be625	9.482

89. Between May 7, 2020 and February 4, 2021, an address analysts have identified as Bitcoin Address 1 received approximately 98 bitcoin (approximately $1,291,600) from the Holding Wallet.[9]

[8] Co-spending is when two or more Bitcoin addresses are used to send bitcoin in a single transaction, which indicates that a single owner holds the private keys for all those addresses. For example, if addresses A and B are co-spent in one transaction, and addresses B and C are co-spent in a second transaction, analysts will conclude that all addresses A, B, and C will belong to the same owner.

[9] Agents conducted undercover purchases at ATMs located in other parts of the state that they believed were, at the time, affiliated with Freeman. Records show that the holding wallet funded some of these ATMs as well. I believe that Freeman no longer operates them and have therefore not discussed them in this affidavit.

90. The following undercover Bitcoin purchases at kiosks operated by Shire Free Church were conducted by FBI or IRS undercover employees:

UC Purchase #	Kiosk Location	Transaction Date	Source of Purchased Bitcoin
1	Red Arrow Diner (A-8)	3/5/2021	Bitcoin Address 1
2	Keene Convenience (A-5)	3/5/2021	Bitcoin Address 1
3	Murphy's Taproom (A-6)	8/4/2020	Bitcoin Address 1
4	Bitcoin Embassy (A-2)[10]	9/9/2020	Bitcoin Address 1
5	Thirsty Owl[11]	9/4/2020	Bitcoin Address 1
8	Thirsty Owl	6/19/2020	Bitcoin Address 1
9	Thirsty Owl	8/25/2020	Bitcoin Address 1

Holding Wallet to LBC/Paxful Accounts

91. Between February 25, 2016 and May 2, 2019, the Holding Wallet sent approximately 2,220 bitcoin (approximately $4,367,770) to a LBC account in the name of Ian B FREEMAN. This LBC account registered the username FTL_Ian using email address ian@freetalklive.com and a New Hampshire driver's license in the name of Ian B Freeman. Between February 26, 2016 and May 2, 2019, the LBC account FTL_Ian completed 3,038 trades with 1,772 other LBC accounts, selling approximately 3,071 BTC for approximately $6,608,500.

92. Additionally, advertisements for this LBC account included options for transactions at kiosks at Murphy's Taproom and Route 101 Goods. Further, the account publicly stated the following information from the accountholder:

> "ABOUT ME: I'm an administrator of Shire BTC, the Shire Free Church's outreach project dedicated to spreading bitcoin in furtherance of our mission to foster peace. All USD and BTC is re-invested in the church's mission. Thanks for being part of it!"

[10] While conducting an undercover purchase from this ATM, investigators noticed security cameras that appear to capture the ATM. The surveillance system and associated hard drives therefore may provide evidence about customers who use the ATM, the operation and control of the ATM, and who empties the cash from the ATM.

[11] I believe that the ATM that was previously at the Thirsty Owl may have been moved to Keene Convenience as the Thirsty Owl is closed for renovations.

93. Between April 11, 2016 and August 7, 2017, the Holding Wallet sent approximately 375 bitcoin (approximately $171,900) that was ultimately deposited to a LBC account in the name of Ian B Freeman. This LBC account registered the username ShireBTC using email address shirebtc+lbc@gmail.com and a New Hampshire driver's license in the name of Ian B Freeman. Between April 14, 2016 and July 5, 2016, the ShireBTC LBC account completed 185 trades with 148 other users, selling approximately 358 BTC for approximately $172,500. Additionally, advertisements for this account included options for transactions at kiosks at Murphy's Taproom, Route 101 Goods, and Thirsty Owl. Further, the account publicly stated the following information from the accountholder:

> "ABOUT US: We are Shire BTC, the Shire Free Church's outreach project dedicated to spreading bitcoin in furtherance of our mission to foster peace. All USD and BTC is re-invested in the church's mission. Thanks for being part of it!"

94. Between October 1, 2019 and December 7, 2020, the Holding Wallet sent approximately 26 bitcoin (approximately $233,490) to a Paxful.com account in the name of Ian B FREEMAN. This Paxful.com account registered the username FTL_Ian using email address ian+pax@freetalklive.com and a New Hampshire driver's license in the name of Ian B Freeman. Between October 4 2019, and December 17, 2020, the account sold approximately 13.45 bitcoin, totaling approximately $154,697 in 64 trades with 38 separate Paxful users.

95. Between March 10, 2016 and May 6, 2016, a Coinbase account in the name of Shire Free Church ending in 0003 sent 40 bitcoin to the Holding Wallet. These transactions were labeled by the Coinbase accountholder as "Church outreach."

96. Between October 1, 2019, and December 7, 2019, the Holding Wallet sent approximately 22.9 bitcoin (approximately $184,200) to a single Bitcoin address. Based on co-spend analysis, this address belongs to the same wallet as the donation address posted on

FreeKeene.com and FreeTalkLive.com, websites associated with Freeman's radio show as of March 10, 2021 (herein, "FK/FTL Wallet"). In fact, the FK/FTL Wallet received approximately 98% of its total bitcoin from the Holding Wallet.

Data Residing on Freeman's ATMs

97. Freeman's ATMs are manufactured by GeneralBytes. GeneralBytes provides the ability for cryptocurrency ATM operators, such as Freeman, to use on servers that the operator maintains. In an April 2018 email exchange with GeneralBytes, Freeman said that he would operate the ATMs from his own server that he runs. This server may be located in Freeman's residence described in Subject Premises A-1.

98. I believe that seizure of the ATMs will allow agents to physically seize transaction log data, configuration data on how the kiosks are set up and communicate with the operator's technical infrastructure, and access data including private encryptions keys that are used to communicate with the server.

99. A review both of the machines themselves and the server could allow investigators to identify, among other things, the amounts of virtual currency sold through the unlawful ATMs and establish ownership and control of the machines.

VII. TRAINING AND EXPERIENCE REGARDING EVIDENCE ASSOCIATED WITH VIRTUAL CURRENCY

100. Because the crimes discussed herein involved the use of virtual currency the items to be seized could be stored almost anywhere within the residences listed in Subject Premises A-1, A-3, A-4, and A-7 (the residences of Nobody (75 Leverett), Freeman (73 Leverett), the Spinellas, Fordham and Rietmann, and DiMezzo respectively) in both physical and electronic formats. These items could also be stored on the persons of these individuals. For example, I am requesting authority to seize bitcoin addresses, bitcoin private keys, bitcoin recovery keys, PGP keys and passwords. Those pieces of data compromise long and complex character strings or words and, in my training and experience, I know that many virtual currency users write down or otherwise record and store such items because they are too long to commit to memory. As such,

these keys, passwords and addresses may be documented in writing and secreted anywhere within a residence or on a person. For all the forgoing reasons, your affiant respectfully submits that probable cause exists to believe that such records, data and documents will be found within the places to be searched, including in computers or on other devices that store electronic data.

101. I also know that people who engage in financial crimes like operating an unlicensed money transmitting business and wire fraud often save bank and financial records for many years and that they often save these records in their residences, especially when they operate the businesses from their residences. The financial crimes these individuals are charged with began in 2015 and I believe that financial records dating back to that year may be kept in the residences to be searched. I also believe that Fordham, Rietmann, and Freeman may save such records in the business they operate described in Subject Premises A-2. I also believe that the targets who operated their virtual currency business through church entities would likely save documents regarding the formation and purpose of those entities in their residences and may keep such documentation for long periods of time. The locations described in A-1 (73 Leverett), A-2, A-3, and A-7 are all either physical or mailing addresses for church entities used in furtherance of the unlawful virtual currency exchange business and therefore I believe that records of those entities and related financial information will be found in those locations. I also believe that people general keep financial documents, money, cash equivalents, and other proceeds of these unlawful schemes in their residence.

102. Individuals involved in digital currency use a variety of digital devices, such as phones and computers. These individuals use multiple digital devices in order to maintain anonymity and to compartmentalize communication, or use encrypted forms of communication in speaking with criminal associates like Freeman's use of Telegram. Additionally, those who use digital currency may store their recovery key or private keys on digital devices, to include phones, computers, laptops, tablets, and hardware wallets. Based on my training and experience, I know that any individual, to include co-conspirators, with access to a cryptocurrency wallet's

recovery key or private keys has the means to transfer the corresponding cryptocurrency held in that wallet. This can be done very quickly.

103. People may also store financial records, photos and videos of co-conspirators or depicting expenditures of money or criminal conduct, contact lists, chats, and other records on digital devices. This also includes personal digital devices that the individual carries on their person. I believe that people who use virtual currency to conduct exchanges on the dark web do so using cell phones and computers.

104. I am aware that Freeman operates a server to run the ATMs. I believe he has used a cellular telephone and has used the phone application Telegram to communicate with customers. In addition, during an interview with a police officer investigating a fraudulent bitcoin purchase in the fall of 2020, Freeman referenced having records of the transaction on his laptop. I have reviewed emails in which Freeman, R. Spinella, A. Spinella, Fordham, and other co-conspirators have discussed their operation of the unlawful virtual currency exchange business.

105. I also know that this business has generated large amounts of cash. I know that people often store cash at their residences, in safes, in safe deposit boxes, and storage units. I also know based on my review of Freeman's emails that he has purchased gold and other cash equivalents that constitute proceeds of his business and that these items are likely to be stored in the same types of places.

VIII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

106. Based on my training and experience, I am aware that businesses frequently use computers to carry out, communicate about, and store records about their business operations. These tasks are frequently accomplished through sending and receiving business-related email and instant messages; drafting other business documents such as spreadsheets and presentations; scheduling business activities; arranging for business travel; storing pictures related to business activities; purchasing and selling supplies online; researching online; and accessing banking, financial, investment, utility, and other accounts concerning the movement and payment of

money online. From my training and experience I know that many smartphones can now function essentially as small computers. They have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and emails, conducting financial activities and storing a vast amount of electronic data.

107. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet.[12] Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data

[12] These statements do not generally apply to data stored in volatile memory such as random-access memory, or "RAM," which data is, generally speaking, deleted once a device is turned off.

in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in

other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime. In addition, decryption of devices and data stored thereon is a constantly evolving field, and law enforcement agencies continuously develop or acquire new methods of decryption, even for devices or data that cannot currently be decrypted.

108. I also know from my training and experience and my review of publicly available materials that several hardware and software manufacturers offer their users the ability to unlock their devices through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint-recognition, face-recognition, iris-recognition, and retina-recognition. Some devices offer a combination of these biometric features and enable the users of such devices to select which features they would like to utilize.

109. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple Inc. ("Apple") offers a feature on some of its phones and laptops called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which on a cell phone is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the phone, and on a laptop is located on the right side of the "Touch Bar" located directly above the keyboard. Fingerprint-recognition features are increasingly common on modern digital devices. For example, for Apple products, all iPhone 5S to iPhone 8 models, as well as iPads (5th generation or later), iPad Pro, iPad Air 2, and iPad mini 3 or later, and MacBook Pro laptops with the Touch Bar are all equipped with Touch ID. Motorola, HTC, LG, and Samsung, among other companies, also produce phones with fingerprint sensors to enable biometric unlock by fingerprint. The fingerprint sensors for these companies have different names but operate similarly to Touch ID.

110. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. To activate the facial-recognition feature, a user must hold the device in front of his or her face. The device's camera analyzes and records data based on the user's facial characteristics. The device is then automatically unlocked if the camera detects a face with characteristics that match those of the registered face. No physical contact by the user with the digital device is necessary for the unlock, but eye contact with the camera is often essential to the proper functioning of these facial-recognition features; thus, a

user must have his or her eyes open during the biometric scan (unless the user previously disabled this requirement). Several companies produce digital devices equipped with a facial-recognition-unlock feature, and all work in a similar manner with different degrees of sophistication, e.g., Samsung's Galaxy S8 (released Spring 2017) and Note8 (released Fall 2017), Apple's iPhone X (released Fall 2017). Apple calls its facial-recognition unlock feature "Face ID." The scan and unlock process for Face ID is almost instantaneous, occurring in approximately one second.

111. While not as prolific on digital devices as fingerprint- and facial-recognition features, both iris- and retina-scanning features exist for securing devices/data. The human iris, like a fingerprint, contains complex patterns that are unique and stable. Iris-recognition technology uses mathematical pattern-recognition techniques to map the iris using infrared light. Similarly, retina scanning casts infrared light into a person's eye to map the unique variations of a person's retinal blood vessels. A user can register one or both eyes to be used to unlock a device with these features. To activate the feature, the user holds the device in front of his or her face while the device directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data from the person's eyes. The device is then unlocked if the camera detects the registered eye. Both the Samsung Galaxy S8 and Note 8 (discussed above) have iris-recognition features. In addition, Microsoft has a product called "Windows Hello" that provides users with a suite of biometric features including fingerprint-, facial-, and iris-unlock features. Windows Hello has both a software and hardware component, and multiple companies manufacture compatible hardware, e.g., attachable infrared cameras or fingerprint sensors, to enable the Windows Hello features on older devices.

112. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

113. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features have been enabled. This can occur when a device has been restarted or inactive, or has not been unlocked for a certain period of time. For example, with Apple's biometric unlock features, these circumstances include when: (1) more than 48 hours has passed since the last time the device was unlocked; (2) the device has not been unlocked via Touch ID or Face ID in eight hours and the passcode or password has not been entered in the last six days; (3) the device has been turned off or restarted; (4) the device has received a remote lock command; (5) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made; or (6) the user has activated "SOS" mode by rapidly clicking the right side button five times or pressing and holding both the side button and either volume button. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time. I do not know the passcodes of the devices likely to be found during the search.

114. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features (such as with Touch ID devices, which can be registered with up to five fingerprints), and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device.

115. For these reasons, if while executing the warrant at Subject Premises A-1, law enforcement personnel encounter a digital device that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to Freeman and Nobody, during the execution of the search and who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that is (a) located at the place searched and (b) falls within the scope of the warrant: (1) compel the use of the person's thumb- and/or fingerprints on the device(s); and (2) hold the device(s) in front of the face of the person with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature. With respect to fingerprint sensor-enabled devices, although I do not know which of the fingers are authorized to access any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors; and, in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

116. If while executing the warrant at Subject Premises A-3, law enforcement personnel encounter a digital device that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to A. Spinella and R. Spinella, during the execution of the search and who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that is (a) located at the place searched and (b) falls within the scope of the warrant: (1) compel the use of the person's thumb- and/or fingerprints on the device(s); and (2) hold the device(s) in front of the face of the person with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature. With respect to fingerprint sensor-enabled devices, although I do not know which of the fingers are authorized to access any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors; and, in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

117. If while executing the warrant at Subject Premises A-4, law enforcement personnel encounter a digital device that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to Fordham and Rietmann, during the execution of the search and who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that is (a) located at the place searched and (b) falls within the scope of the warrant: (1) compel the use of the person's thumb- and/or fingerprints on the device(s); and (2) hold the device(s) in front of the face of the person with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature. With respect to fingerprint sensor-enabled devices, although I do not know which of the fingers are authorized to access any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors; and, in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

118. If while executing the warrant at Subject Premises A-7, law enforcement personnel encounter a digital device that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to DiMezzo, during the execution of the search and who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that is (a) located at the place searched and (b) falls within the scope of the warrant: (1) compel the use of the person's thumb- and/or fingerprints on the device(s); and (2) hold the device(s) in front of the face of the person with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature. With respect to fingerprint sensor-enabled devices, although I do not know which of the fingers are authorized to access any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors; and, in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

119. The proposed warrant does not authorize law enforcement to compel that an individual present at the Subject Premises state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to compel an individual present at the Subject Premises to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Devices.

IX. CONCLUSION

120. For all the reasons described above, there is probable cause to believe that evidence of violations of 18 U.S.C. §§ 1960, 371 (prohibition of unlicensed money transmitting business and conspiracy), 18 U.S.C. §§ 1343, 1349 (conspiracy to commit wire fraud and wire fraud), 18 U.S.C. § 1956(a) (laundering of monetary instruments, including funds represented to be proceeds of specified unlawful activity), 31 U.S.C. §§ 5313(a) and 5322 (failure to file currency transaction reports ("CTRs")), and 31 U.S.C. § 5318(h) and 5322 (failure to maintain an effective anti-money laundering program) (collectively, the "Subject Offenses"), as described above in Attachments B-1 through B-15 of this affidavit will be found in a search of **SUBJECT PREMISES A-1 through A-15** as further described above and in Attachments A-1 to A-15 of this affidavit.

Respectfully Submitted,

/s/ Kathryn Thibault
Kathryn Thibault
Special Agent, Federal Bureau of Investigation

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: **Mar 15, 2021**
Time: **3:48 PM, Mar 15, 2021**

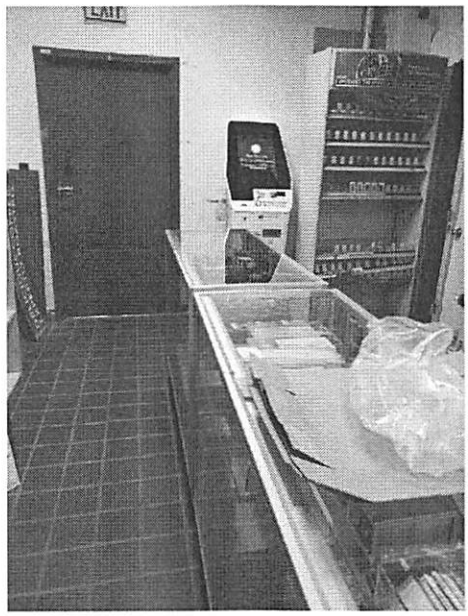
Andrea K. Johnstone

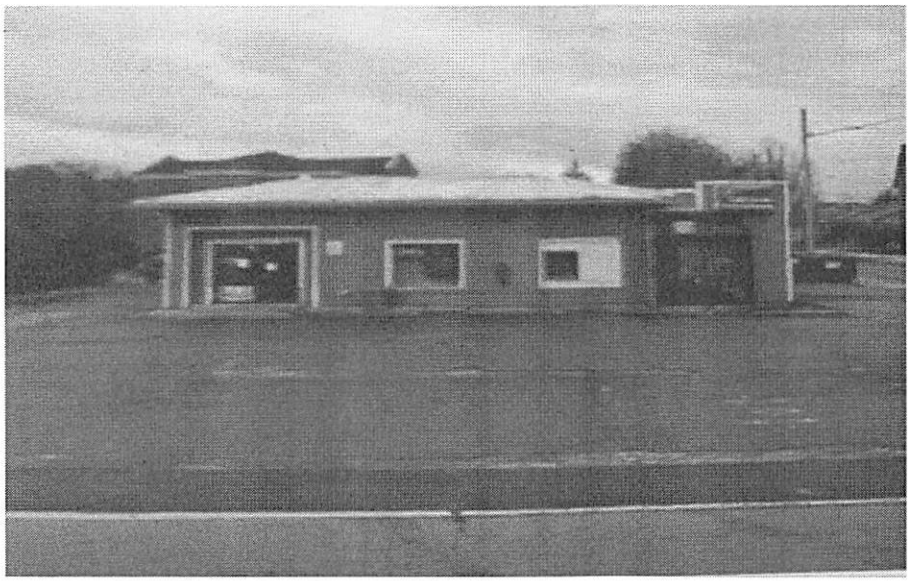
HONORABLE ANDREA K. JOHNSTONE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-5

Campus Convenience, 152 Winchester St., Keene, New Hampshire

The Subject Premises is a one level commercial building, green in color, sits in a paved parking lot on Winchester Street. The building has a main entrance for the general public on the left front corner of the building that consists of two glass doors. To the right of the front entrance are two glass panel/windows that contain neon "open" signs. On the far front right corner is a vestibule employee entrance. There is customer parking surrounding the entire structure. There is a large black dumpster to the rear of the building on the right side.





ATTACHMENT B-5

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1960 (prohibition of unlicensed money transmitting business), 18 U.S.C. § 1956(a) (laundering of monetary instruments, including funds represented to be proceeds of specified unlawful activity), 31 U.S.C. § 5313(a) and 5322 (failure to file currency transaction reports ("CTRs"), and 31 U.S.C. § 5318(h) and 5322 (failure to maintain an effective anti-money laundering program) (collectively, the "Subject Offenses"), including:

a. Virtual Currency ATM machine and including the following stored in the ATM machine:

i. United States currency, digital currency such as Bitcoin stored on electronic wallets or other means.

ii. Records of all transactions.

iii. Programs reflecting transactions that occurred using the machine.

iv. Materials used to operate the machine.

i. Any digital device used to facilitate the above-listed violations within the ATM machine and forensic copies thereof.

b. With respect to any digital device used to facilitate the above-listed violations within the ATM machine or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious

software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.